REMARKS

I. Amendments to the Claims

Applicant amends claims 26-30, 32, 33, 36-45, and 48-50. The amendments are supported by Applicant's specification at, for example, page 5, lines 16-20; page 6, lines 25-27; and page 7, lines 8-11, among other places. Claims 26-50 are pending and under examination.

II. Office Action

Applicant traverses the objection and rejections set forth in the Office Action, wherein the Examiner:

(1) objected to the drawings;

(2) rejected claims 26-37 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter;

(3) rejected claims 26-28, 30-32, 35-44, and 47-50 under 35 U.S.C. § 102(a) as being anticipated by European Publication No. EP 1330095 A1 ("Lahtinen");

(4) rejected claim 29 under 35 U.S.C. § 103(a) as being unpatentable over Lahtinen in view of U.S. Patent Application Pub. No. 2003/0149888 A1 ("Yadav"); and

(5) rejected claims 33, 34, 45, and 46[1] under 35 U.S.C. § 103(a) as being unpatentable over Lahtinen in view of U.S. Patent Application Pub. No. 2002/0105910 ("Maher").

III. Response to Objection and Rejections

Applicant respectfully traverses the aforementioned objections and rejections, and requests reconsideration based on the following remarks.

A. Objection to the Drawings

The Office Action objected to the drawings because they "[lack] description or content for the corresponding reference numbers." Office Action, p. 2. Specifically, the Examiner

[1] The Office Action, on page 11 under item 12, lists claim 29 under this rejection; however, in the ensuing explanation, the Office Action instead rejects claims 33, 34, 45, and 46.

requires "[b]rief description of the corresponding reference numbers ... in empty boxes." *Id.* In response, Applicant submits the attached five (5) replacement drawing sheets (containing Figs. 1-5), in which descriptive labels have been added to the boxes or arrows corresponding to reference numbers 12, 14, 16, 18, 44, 46, 48, 50, 52, 54, 56, 58, 60, 72, and 74-81 in Figs. 1-5. The added labels are supported by the description in Applicant's specification for each box or arrow. Accordingly, Applicant respectfully requests withdrawal of the objection.

B. Claim rejections under 35 U.S.C. § 101

Applicant requests reconsideration and withdrawal of the rejection of claim 26-37 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Specifically, the Office Action alleged that "the body of the claim does not positively recited any elements of hardware." Office Action, p. 4. In response, and without conceding to the Examiner's arguments regarding alleged non-statutory subject matter, Applicant has amended claim 26 to recite that the claimed intrusion detection system is implemented using one or more computers. Applicant deems the rejection of claim 26 under § 101 overcome, and requests its withdrawal. Claims 27-37 depend from claim 26, incorporate the recitations of claim 26, and therefore overcome the § 101 rejection for at least the same reason. Accordingly, Applicant respectfully requests withdrawal of the § 101 rejection.

C. Claim rejections under 35 U.S.C. § 102(a)

Applicant requests reconsideration and withdrawal of the rejection of claims 26-28, 30-32, 35-44, and 47-50 under 35 U.S.C. § 102(a) as being anticipated by Lahtinen. In order to establish anticipation under 35 U.S.C. § 102, the Federal Circuit has held that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of*

California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). *See also* M.P.E.P. § 2131. Here, Lahtinen does not disclose each and every element of at least independent claims 26 and 38.

Independent Claim 26

Regarding independent claim 26, Lahtinen does not disclose or suggest at least Applicant's claimed

> intrusion detection system ... comprising:
> ...
> a pattern matching engine for ... comparing the captured data with attack signatures for generating an event when a match between the captured data and at least one attack signature is found; and
>
> a response analysis engine, triggered by said event, for comparing with response signatures response data being transmitted on said network ... and for correlating results of said comparisons with attack and response signatures for generating an alarm,

as recited in claim 26 (emphases added). Specifically, Lahtinen does not disclose or suggest that a response engine is triggered by an event generated by a pattern matching engine.

In its assertion to the contrary, on page 5, the Office Action cited "analysis of response-request pairs," and Lahtinen's paragraph [0044]. The analysis of request-response pair described in Lahtinen, however, does not disclose or suggest the above-quoted features of claim 26.

Lahtinen is instead directed to "monitoring the flow of a data stream traveling between a client and a server system," (Lahtinen, par. [0001]), and detecting an intrusion initiating from a client (as a request) and targeting a server, which may send a response to the client (*see*

Lahtinen, par. [0003]). Lahtinen describes an "HTTP proxy which can filter the request-response pairs … [as a] security solution." *Id.*, par. [0009].

In Lahtinen, a response from a server to a client is analyzed irrespective of any event by a pattern matching engine. In the excerpts cited by the Office Action, Lahtinen states that:

> If a proxy system is used, the analysis of the response-request pairs according to the present invention would be carried out for the request 184 and response 190 [see Lahtinen, Fig. 1B], and so on for further communications as well, or alternatively for the traffic between the proxy and the web server … In general, information contained in the request 316 is passed to the analysis system 300 [see Id., Fig. 3]. The first inspection block 206 checks the host and client identifiers and possible common parameters, and stores them in the corresponding table 250. It may also perform a limitation check and a fingerprinting procedure in order to find malicious requests, classify and report events, etc., as described above with reference to FIG. 2. The first inspection block 206 analyzes the request in its descriptor identification block 226. If the request is the first one, it can only be checked against fingerprints and the limitations file 252.
>
> The response 318 is analyzed as well. The second inspection block 266 performs tasks similar to the first inspection block 206 in the sense that it analyzes the HTML part of the stream and tries to identify possible descriptors and limitations. The descriptors identified are stored in the table of available states 251. Similarly, the limitations identified are stored in the limitations file 252.

Id., pars. [0044]-[0045] (emphasis added). This portion of Lahtinen describes the process of analyzing response-request pairs for a proxy system. More specifically, regarding the process of sending data to inspection block 266, Lahtinen explains:

> The data stream traveling from the server 152 to the user agent 150 is analyzed as well. For this purpose, it is possible to use an inspecting block 266 … The receiving block 262 receives the data stream coming from the server. It forwards it to the control block 264, which operates in much the same way as the control block 204 does … The control block forwards the content HTTP stream to the inspection block 266.

Id., pars. [0035]-[0037] (emphases added). Therefore, in Lahtinen, response 318 [from a server to a client] is analyzed irrespective of any event by a pattern matching engine. Lahtinen thus does not disclose or suggest that "a pattern matching engine … [compares] the captured data with attack signatures for generating an event when a match between the captured data and at

least one attack signature is found; and a response analysis engine [is] triggered by said event [to compare] with response signatures response data being transmitted on said network," as recited in claim 26 (emphasis added).

Independent Claim 38

Regarding independent claim 38, Lahtinen does not disclose or suggest Applicant's claimed method for detecting unauthorised use of a network, which comprises

> capturing data being transmitted on said network;
>
> comparing the captured data with attack signatures for generating an event when a match between the captured data and at least one attack signature is found; and
>
> when triggered by said event:
> comparing with response signatures response data being transmitted on said network as a response to said data matched with said at least one attack signature; and
>
> correlating results of said comparisons with attack and response signatures for generating an alarm,

as recited in claim 38 (emphases added).

In its assertion to the contrary, the Office Action, on page 8, cited "matching the data stream against known misuse patterns," in Lahtinen's paragraph [0016], and "generating an alarm event," in Lahtinen's paragraph [0018]. The above cited portions of Lahtinen do not disclose or suggest the above-quoted features of claim 38.

In the above cited sections and the related excerpts, Lahtinen explains that

> [i]n the monitoring process, a data stream traveling from the server to the client is analyzed in order to identify at least one response descriptor in the data stream. Identified response descriptors are stored in a set of available states for the client. Next, a data stream traveling from the client to the server is analyzed in order to identify at least one request descriptor. Identified request descriptors are compared with the set of available states for said client, and responsive to the comparing step, a monitoring result is generated. Id., [0014] (emphases added).
>
> [T]he monitoring may further include performing a predermined [sic] action at least partially based on the monitoring result. *Id.*, par. [0015].

> [S]aid predetermined action may include matching the data stream [travelling from the client to the server] against known misuse patterns, if at least one request descriptor fails to match the stored response descriptors in the set of available states. *Id.*, par. [0016].
>
> [S]aid predetermined action may include generating an alarm event, which is selected at least partially based on the monitoring result. *Id.*, par. [0018].

Lahtinen thus teaches analyzing data streams, i.e., responses, sent from a server to a client in order to identify possible requests that the client can later send to the server, when the client replies to the server's response. After that, Lahtinen monitors the requests that the client sends to the server. If a future request fails to match one of those possible requests, Lahtinen may further examine that request by matching it against known misuse patterns. Alternatively, Lahtinen may generate an alarm event. Thus, Lahtinen analyzes the server response as part of its monitoring process (*see also* Lahtinen, pars. [0053]-[0063]) and does not disclose or suggest at least Applicant's claimed "when triggered by an event" generated "when a match between the captured data and at least one attack signature is found," as recited in independent claim 38. Moreover, Lahtinen generates its alarm event as a result of monitoring the requests sent from client to server, and not upon "correlating results of said comparisons with attack and response signatures," as recited in claim 38.

Dependent Claims 27, 28, 30-32, 35-37, 39-44, and 47-50

The Office Action, on pages 5-10, asserted that Lahtinen teaches or suggests each and every element of each the above claims. Applicant, however, respectfully disagrees. To begin, as explained above in relation to claims 26 and 38, Lahtinen does not anticipate the above claims, by virtue of their dependence, either directly or indirectly, from one of claims 26 and 38.

Moreover, regarding claims 30 and 42, the Office Action, on page 6, asserted paragraph [0044] of Lahtinen discloses that the "response analysis engine generates the alarm when said response data indicates that a new network connection has been established," as recited in claims

30 and 42. Applicant, however, respectfully disagrees, and contends that Lahtinen does not teach or suggest this feature. Specifically, paragraph [0044] of Lahtinen describes the analysis of response-request pairs by the proxy system, and does not indicate that an alarm is generated as a result of establishment of a new network connection, and the Office Action failed to point to any specific excerpt where it does.

Further, regarding claims 31 and 43, the Office Action, on page 6, asserted that paragraph [0032] of Lahtinen discloses the recited features that the "response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic," by disclosing "a table of available state, and legitimate/valid," as quoted by the Office Action. Applicant, however, respectfully disagrees, and contends that Lahtinen does not teach or suggest the recited features. Specifically, paragraph [0032] of Lahtinen describes "a table of available states 251, which contains descriptors, i.e. what kind of legitimate/valid requests may be coming from the client" (emphasis added). Therefore, Lahtinen discloses determining legitimate requests from client and not categories for response signatures, as explained above.

Regarding claim 36, Applicant contends that Lahtinen does not teach or suggest the recited features that a probing task

> generates the alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine; or
> ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine.

In its assertion to the contrary, the Office Action cited Fig. 1B and paragraph [0009] in Lahtinen. However, neither Fig. 1B nor paragraph [0009] in Lahtinen does teach or suggest that a probing

task generates an alarm if only response signatures indicating legitimate traffic have been used, and the Office Action failed to point to an excerpt that does so disclose.

Since Lahtinen does not disclose each and every element of independent claims 27 and 38, Lahtinen does not anticipate Applicant's claims 27 and 38 under 35 U.S.C. § 102(a). Therefore, independent claims 27 and 38 should be allowable, along with dependent claims 27, 28, 30-32, 35-37, 39-44, and 47-50. Accordingly, Applicant respectfully requests withdrawal of the 35 U.S.C. § 102(a) rejection.

D. Claim rejections under 35 U.S.C. § 103(a)

Applicant requests reconsideration and withdrawal of the remaining rejections of claims 29, 33, 34, 45, and 46 under 35 U.S.C. § 103(a) as being unpatentable over Lahtinen in view of one or more of Yadav and Maher.

The Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective obviousness analysis. *See* M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 USPQ2d 1385 (2007). Specifically, the Office Action has not properly ascertained the differences between the claimed invention and the prior art, at least because it has not interpreted the prior art and considered *both* the invention *and* the prior art *as a whole*. See M.P.E.P. § 2141(II)(B).

Applicant has previously established herein that Lahtinen does not teach or suggest each and every element of independent claims 27 and 38. The Office Action's application of Lahtinen alone or in combination with one or more of Yadav and Maher against the dependent claims does not cure the deficiencies of Lahtinen as to independent claims 27 and 38. The Office Action's

allegations as to Lahtinen and the secondary references with regard to the dependent claims does not address the failure of Lahtinen to teach or suggest each and every element of the independent claims, as explained in the previous section.

Specifically, on pages 10-11, the Office Action rejected claim 29 as being unpatentable over Lahtinen in view of Yadav. Further, on pages 11-12, the Office Action rejected claims 33, 34, 45, and 46, as being unpatentable over Lahtinen in view of Maher. In each rejection, the Office Action relied on Lahtinen to disclose all features of one of claims 26 and 38 from which the rejected claim depends, and further cited Yadav or Maher for the disclosure of additional features recited in the dependent claims. Regardless of whether Yadav and Maher disclose the features for which the Office Action relied on as to the dependent claims, which the Applicant does not concede, Yadav and Maher do not cure the deficiencies of Lahtinen, because they do not teach or suggest those features of claims 26 and 38 which are missing from Lahtinen.

Dependent claims 29, 33, 34, 45, and 46 are therefore nonobvious and should be allowable at least by virtue of their respective dependence from base claim 27 or 38. Applicant therefore requests withdrawal of the remaining 35 U.S.C. § 103(a) rejections.

IV. Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully requests the reconsideration and withdrawal of the rejections, and the timely allowance of the pending claims.

The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

If there are any remaining issues or misunderstandings, Applicant requests the Examiner telephone the undersigned representative to discuss them.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 21, 2009

By: /David M. Longo/
David M. Longo
Reg. No. 53,235

/direct telephone: (571) 203-2763